



---

## MOSS Rules of Behavior

*September 26, 2008*

---

*Prepared By:*

**Enterprise Collaboration Services (ECS)**  
*IRM/OPS/SIO/API/ECS*



## 1. Introduction

The Office of Management and Budget (OMB) Circular A-130, Appendix III Security of Federal Automated Information Resources requires that 'Rules of Behavior' be established for each general support information technology system and major application processing government information. The "Rules of Behavior" delineated below pertain to all persons who utilize the DoS SharePoint Services (DOSSS) web portal which is an IT resource for the Department of State. The following Rules of Behavior and acceptable use policy apply to all administrators and contributors of the DoS SharePoint Services environment whether DoS employees, contractors or external agencies.

The Rules of Behavior provide general instructions on the appropriate use of the Department's SharePoint resource and apply to users and specifically apply to the following SharePoint sites and their respective sub-sites:

- SharePoint Bureau and Post Sites ( <http://collaborate.state.gov> )

These sites may be on any of the following networks:

- SharePoint OpenNet
- SharePoint OpenNet Demilitarized Zone (DMZ)
- SharePoint ClassNet
- SharePoint ClassNet Demilitarized Zone (DMZ)
- Groove OpenNet
- Groove ClassNet

## 2. Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy or guidelines. Rather, they are intended to supplement the DoS Information Security Program Policy and the DoS Information Security Program Handbook. Because written guidance cannot cover every contingency, Department staff is asked to augment these rules and use their best judgment and highest ethical standards to guide their actions.

As with any intranet website users must adhere to the following DoS website guidelines: [5FAH-8 H-100](#) , [5FAH-8 H-200](#) , [5FAH-8 H-400](#) , [5FAH-8 H-430](#) , [5FAH-8 H450](#)

Additionally for internet hosted sites users must adhere to the following Guidelines for Public Information Dissemination on the Internet: <http://isc.state.go>

## 3. Enterprise Collaboration Services SharePoint Overview

SharePoint allows you to:

- Store your organization's documents and information securely
- Collaborate on documents and reports
- Manage content and streamline processes
- Build a collaboration and published website for information sharing and or marketing purposes
- Search for documents, sites and SMART Archival Messages
- Share information and collaborate internally (within DoS on ClassNet and OpenNet) and externally (with external agencies on SiproNet and NiproNet) across network boundaries

## 4. SharePoint Rules of Behavior

4.1. Administrators must be assigned by Bureau or Office advocates.

4.2. Contributors and users must be assigned by the site administrator.

4.3. Administrators can give contributor access to those individuals that have agreed to the ROB and require the use of SharePoint to solve a business need.

4.4. Users must follow a Configuration Management process for storing information and data on the SharePoint sites.

4.5. Administrators is responsible for the management of site content at the parent site level and at the sub-site levels. Administrators may re-assign the responsibility of Content Manager to those individuals who manage particular sub-sites.

4.6. Users can not post combinations of key Privacy Information or combinations of Personally Identifiable Information (PII).

4.6.1. These combinations could include full name, birth date, social security number, address.

4.7. Users should not post items that will affect the National Security of the Department of State or any collaborating agencies.

4.7.1.1. Examples of Non-Acceptable Information include: Social Security Number + Last Name (or any combination of SSN with other PII, i.e. date of birth, phone number, first name)

4.7.1.2. Communications or contracts regarding negotiations regarding external affairs

4.7.1.3. Architectural drawings or floor plans related to DoS facility (embassies, , consulates, posts, etc.)

4.8. Users should not publicly store DoS employee's personnel records

4.8.1. Examples of personnel records include compensations, rewards, reviews or appraisals.

4.9. Users who violate or observe a user that is in violation of the ROB will/should be reported to your local ISSO.

## **5. Non-Acceptable Uses**

This policy identifies actions that should not be performed with SharePoint.

- It is strictly prohibited to review process or modify Personally Identifiable Information (PII), electronic protected health information or other delicate information while working within a SharePoint site. For more information on PII, please visit the Bureau of Administration's website regarding Privacy Matters: <http://a.state.gov/content/privacymatters/index.asp>
- SharePoint should not be used to post inappropriate documentation, announcements, lists, etc. that could be considered offensive by other site participants.
- Cross enclave (OpenNet to ClassNet and vice versa) use of SharePoint is not supported.